INTELLIGENCE BRIEFING
Security Command Center

TLP:CLEAR
2026-03-31 06:18 UTC

# Threat Actor Impersonates CERT-UA to Deploy RAT on Ukrainian Government and Hospital Networks

THREAT CAMPAIGN | CRITICAL | CVSS 8.1

| | |
|---|---|
| **SCC Item ID** | SCC-CAM-2026-0126 |
| **Type** | Threat Campaign |
| **Severity** | CRITICAL |
| **CVSS Base Score** | 8.1 |
| **Affected Products** | Ukrainian government agency networks and hospital networks |
| **Published** | 2026-03-30 |
| **Discovery Source** | Gemini |

## Executive Summary

An unattributed threat actor impersonated CERT-UA, Ukraine's national computer emergency response team, to deliver a Remote Access Trojan (RAT) against Ukrainian government agencies and hospital networks. The campaign exploits trust in official cybersecurity communications to bypass user skepticism, enabling persistent attacker access to sensitive government and healthcare systems. Organizations supporting Ukrainian operations, exchanging threat intelligence with CERT-UA, or operating in adjacent sectors should treat this as an active social engineering threat requiring immediate staff awareness and email verification controls.

## Technical Analysis

The campaign uses impersonation of CERT-UA correspondence as the delivery mechanism (T1036, T1036.005, CWE-290: Authentication Bypass by Spoofing; CWE-1021: Improper Restriction of Rendered UI Layers) to deliver phishing lures (T1566, T1566.001) that install a Remote Access Trojan on victim endpoints. Once deployed, the RAT establishes C2 communications over standard application-layer protocols (T1071.001), supports ingress tool transfer for additional payload staging (T1105), and may use valid or compromised accounts for lateral movement (T1078). Remote access capability is maintained via T1219. No CVE identifier applies to this campaign-level event. No specific RAT family, malware hash, C2 infrastructure, or patch has been publicly identified in available reporting. Attribution remains unestablished. Source quality score is 0.472, reflecting reliance on secondary and tertiary reporting; technical specifics should be treated as unverified until confirmed by CERT-UA or a primary threat intelligence source.

## Action Checklist

1. Containment, Alert staff across government and healthcare IT teams that CERT-UA communications are being spoofed. Instruct personnel to verify any inbound CERT-UA correspondence by calling CERT-UA directly through official contact channels before opening attachments or clicking links. Temporarily flag and hold for review any inbound email claiming to originate from CERT-UA or Ukrainian government cybersecurity bodies.

2. Detection, Search email gateway logs for messages with sender domains that spoof or closely resemble cert.gov.ua. Review endpoint logs for unusual process creation from email clients or document applications (e.g., Outlook, Word spawning cmd.exe, powershell.exe, or wscript.exe). Query EDR telemetry for outbound connections to newly registered or low-reputation domains following document open events. Look for T1071.001 indicators: unexpected HTTP/HTTPS beaconing to external hosts from workstations that do not normally initiate such connections.

3. Eradication, Isolate any endpoint showing RAT behavioral indicators (persistent outbound beaconing, unexpected scheduled tasks, new autorun registry entries, or remote access tool artifacts). Revoke and rotate credentials for any accounts active on suspected compromised systems. Block identified C2 domains and IPs at perimeter and DNS if IOCs become available from CERT-UA advisories.

4. Recovery, After isolation and credential rotation, reimage compromised endpoints rather than attempting in-place remediation, given RAT persistence mechanisms. Validate that no scheduled tasks, registry run keys, or startup folder entries remain from the infection. Monitor previously compromised accounts and systems for 30 days post-remediation for re-infection indicators.

5. Post-Incident, Conduct a phishing simulation specifically using authority impersonation scenarios (mimicking CERT-UA or equivalent national CERT bodies) to assess staff susceptibility. Implement DMARC, DKIM, and SPF enforcement on inbound mail gateways to reduce spoofed-sender delivery. Establish a verified out-of-band contact procedure for all inbound threat advisories from external authorities before any attachment or link is actioned. Map control gaps to NIST SP 800-53 AT-2 (Literacy Training and Awareness), SI-8 (Spam Protection), and SC-7 (Boundary Protection).

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |
| **Escalation Criteria** | Escalate immediately to national CERT, senior leadership, and legal/privacy counsel if any compromised endpoint belongs to a healthcare network with access to patient records (PHI), if Active Directory logs show the RAT operator has authenticated with harvested credentials to additional systems beyond the initial lure-opened workstation, or if C2 traffic patterns suggest active operator-directed collection rather than automated beaconing — all conditions indicating the blast radius has expanded beyond the initial foothold. |

| | |
|---|---|
| **Recovery Notes** | After reimaging compromised endpoints and rotating all credentials active on those systems, validate email gateway DMARC enforcement is in 'p=reject' policy (not 'p=none' monitor mode) before returning affected users to normal operations, as the initial attack vector remains live while the campaign is active. Monitor recovered accounts for 30 days using Windows Security Event ID 4624 (Logon) and 4768/4769 (Kerberos ticket requests) for anomalous authentication times, source IPs, or service access patterns that would indicate the threat actor retained access via a second persistence mechanism not identified during eradication. Given the government and hospital network scope, retain all forensic images and evidence for a minimum of 90 days to support any law enforcement referral or regulatory breach notification process. |
| **Forensic Artifacts** | Spoofed CERT-UA email messages (.eml format) with full SMTP headers preserved — specifically the Received chain, X-Originating-IP, DKIM-Signature (or its absence), and MIME-From vs envelope-From mismatch that characterizes this sender spoofing technique \| Sysmon Event ID 1 (Process Create) logs capturing the process lineage of Outlook.exe or Winword.exe spawning cmd.exe, powershell.exe, wscript.exe, or mshta.exe at the moment the lure document was opened — the primary execution indicator for this socially-engineered RAT delivery chain \| RAT binary and dropped lure document preserved from %TEMP%, %APPDATA%, or user Downloads directory — the RAT delivered via this campaign will have a file creation timestamp correlating with the document-open event, and may include a decoy document displayed to the victim to reduce suspicion \| Windows Registry persistence keys (HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM equivalent) and scheduled task XML definitions exported from C:\Windows\System32\Tasks\ — the primary persistence mechanisms for RATs delivered via spearphishing document lures targeting government workstations \| DNS query logs and proxy/gateway logs showing outbound resolution and HTTP/HTTPS connections to C2 infrastructure following document-open timestamps — Sysmon Event ID 3 (Network Connection) or gateway NetFlow records capturing the T1071.001 beaconing pattern to newly registered domains are critical for mapping the full C2 infrastructure used in this CERT-UA impersonation campaign |

### Per-Action IR Details

**Containment — Alert staff across government and healthcare IT teams that CERT-UA communications are being spoofed. Instruct personnel to verify any inbound CERT-UA correspondence by calling CERT-UA directly through official contact channels before opening attachments or clicking links. Temporarily flag and hold for review any inbound email claiming to originate from CERT-UA or Ukrainian government cybersecurity bodies.**

**NIST Phase:** Containment

**Reference:** NIST 800-61r3 §3.3 — Containment Strategy (CSF RS.MA-01: Execute IR plan, contain, communicate)

**Controls:** NIST IR-4 (Incident Handling), NIST IR-6 (Incident Reporting), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 4.4 (Implement and Manage a Firewall on Servers)

**Compensating:** For teams without a mail gateway quarantine feature: deploy a Microsoft Exchange transport rule (New-TransportRule in EMS) or Postfix header_checks rule that holds any inbound message where the From header contains 'cert.gov.ua' but the envelope sender domain does not match — flagging it for manual review. Distribute an emergency staff notice via out-of-band channel (Signal or phone tree) rather than email, since the attack vector is email itself.

**Evidence:** Before quarantining held messages, export raw .eml files from the mail gateway queue preserving full SMTP headers (Received, X-Originating-IP, DKIM-Signature fields) to document the spoofed sender infrastructure. Capture mail gateway or MTA delivery logs (Postfix maillog, Exchange Message Tracking Log via Get-MessageTrackingLog) showing the originating IP, envelope From, and MIME From for each flagged message — this establishes the sender spoofing pattern specific to this CERT-UA impersonation campaign.

**Detection — Search email gateway logs for messages with sender domains that spoof or closely resemble cert.gov.ua. Review endpoint logs for unusual process creation from email clients or document applications (e.g., Outlook, Word spawning cmd.exe, powershell.exe, or wscript.exe). Query EDR telemetry for outbound connections to newly registered or low-reputation domains following document open events. Look for T1071.001 indicators: unexpected HTTP/HTTPS beaconing to external hosts from workstations that do not normally initiate such connections.**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.2 — Detection and Analysis (CSF DE.AE-02, DE.AE-03, DE.AE-07: Correlate events, integrate CTI, analyze adverse activity)

**Controls:** NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs)

**Compensating:** Without EDR: deploy Sysmon with SwiftOnSecurity config (Event ID 1 — Process Create, Event ID 3 — Network Connection, Event ID 11 — FileCreate). Query Windows Security Event Log for Event ID 4688 (Process Creation) filtering on ParentProcessName matching OUTLOOK.EXE or WINWORD.EXE with ChildProcessName matching cmd.exe, powershell.exe, wscript.exe, or mshta.exe. For network beaconing detection without a SIEM, run the Sigma rule 'proc_creation_win_malware_rat' against collected Sysmon logs using sigmac converted to PowerShell, and capture outbound DNS queries using Wireshark or tcpdump on the gateway filtered for newly registered domains (WHOIS age < 30 days).

**Evidence:** Capture Sysmon Event ID 1 logs showing the full process lineage (parent: Outlook/Word → child: cmd/PowerShell/wscript) including command-line arguments before any remediation action. Preserve Windows Security Event Log Event ID 4688 entries and DNS query logs (Windows DNS debug log or gateway resolver cache) showing resolution of C2 domains immediately after document open timestamps. Export email gateway logs (Exchange Message Tracking or Postfix maillog) for all cert.gov.ua lookalike domains including homoglyph variants (e.g., cert.g0v.ua, cert-gov.ua, cert.gov.ua.attacker.com) to map the full sender infrastructure used in this impersonation campaign.

**Eradication — Isolate any endpoint showing RAT behavioral indicators (persistent outbound beaconing, unexpected scheduled tasks, new autorun registry entries, or remote access tool artifacts). Revoke and rotate credentials for any accounts active on suspected compromised systems. Block identified C2 domains and IPs at perimeter and DNS if IOCs become available from CERT-UA advisories.**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication (CSF RS.MA-01: Mitigate, remove threat from environment, verify eradication)

**Controls:** NIST IR-4 (Incident Handling), NIST SI-3 (Malicious Code Protection), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-9 (Protection of Audit Information), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 5.3 (Disable Dormant Accounts)

**Compensating:** Without enterprise EDR for isolation: use Windows Firewall (netsh advfirewall set allprofiles firewallpolicy blockinbound,blockoutbound) to immediately cut outbound connectivity on the suspected host while preserving it for forensic collection. For RAT persistence enumeration without EDR, run Autoruns (Sysinternals) to enumerate all HKCU\Software\Microsoft\Windows\CurrentVersion\Run, HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, scheduled tasks, and startup folder entries — export to CSV and diff against a known-good baseline. Use osquery (SELECT * FROM scheduled_tasks; SELECT * FROM registry WHERE key LIKE '%CurrentVersion\Run%') for cross-host sweep if osquery is deployed.

**Evidence:** Before isolating the endpoint, acquire a volatile memory image using WinPmem or DumpIt to capture the live RAT process, injected threads, and active C2 socket connections — this impersonation campaign's RAT will leave artifacts in memory (injected DLLs, hollowed processes, open handles to C2 sockets) that disappear on reboot. Preserve the following persistence artifacts prior to remediation: contents of HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM\...\Run registry keys, %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup folder contents, and output of 'schtasks /query /fo LIST /v' — these are the primary RAT installation footprints for socially-engineered RAT delivery via document lure.

**Recovery — After isolation and credential rotation, reimage compromised endpoints rather than attempting in-place remediation, given RAT persistence mechanisms. Validate that no scheduled tasks, registry run keys, or startup folder entries remain from the infection. Monitor previously compromised accounts and systems for 30 days post-remediation for re-infection indicators.**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery (CSF RC: Execute recovery plan, restore systems, verify integrity, communicate)

**Controls:** NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP (Contingency Planning — system restore procedures), CIS 4.6 (Securely Manage Enterprise Assets and Software)

**Compensating:** For teams without enterprise imaging infrastructure: use a verified, offline Windows installation media to perform a clean OS reinstall, validating the install media hash against Microsoft's published checksums before use. Post-reimage, validate system integrity using the free Sysinternals Sigcheck tool against all binaries in %SYSTEM32% and %PROGRAMFILES% to detect any RAT components that survived via firmware or alternate data streams. Deploy Sysmon on the recovered host immediately post-reimage to establish a clean behavioral baseline before reconnecting to the network.

**Evidence:** Before reimaging, collect a forensic disk image (FTK Imager Lite or dcfldd) of the compromised endpoint to preserve the RAT binary, dropped lure documents, browser history (for C2 domain reconnaissance), and prefetch files (%SYSTEMROOT%\Prefetch) that record execution timestamps of RAT components — this evidence is required for post-incident root cause analysis and any potential attribution or law enforcement referral given that the targets are government and healthcare networks. Document all active user sessions (qwinsta /server) and mapped network drives at time of isolation to identify potential lateral movement scope before imaging.

**Post-Incident — Conduct a phishing simulation specifically using authority impersonation scenarios (mimicking CERT-UA or equivalent national CERT bodies) to assess staff susceptibility. Implement DMARC, DKIM, and SPF enforcement on inbound mail gateways to reduce spoofed-sender delivery. Establish a verified out-of-band contact procedure for all inbound threat advisories from external authorities before any attachment or link is actioned. Map control gaps to NIST SP 800-53 AT-2 (Literacy Training and Awareness), SI-8 (Spam Protection), and SC-7 (Boundary Protection).**

**NIST Phase:** Post Incident

**Reference:** NIST 800-61r3 §4 — Post-Incident Activity (CSF GV, ID: Lessons learned, update policies, improve detection, share intelligence)

**Controls:** NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-2 (Incident Response Training), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

**Compensating:** DMARC/DKIM/SPF enforcement requires only DNS TXT record changes — zero-cost for any organization controlling their DNS zone. Use MXToolbox (mxtoolbox.com/dmarc) to validate records post-deployment. For phishing simulations without a commercial platform, use the free GoPhish framework (getgophish.com) to build authority-impersonation lure templates that mimic this campaign's CERT-UA pretext. For the out-of-band verification procedure, publish CERT-UA's verified phone number and PGP key fingerprint on a printed, physically posted reference sheet in each IT operations area — removing dependency on any email-delivered contact information that could itself be spoofed.

**Evidence:** Collect and retain the following for the post-incident review: (1) all quarantined spoofed CERT-UA emails with full headers as evidence of the impersonation TTP, (2) Sysmon/Event ID 4688 logs documenting which users opened lure documents and the resulting child process tree, (3) DNS resolution logs showing C2 domain queries from any compromised host, and (4) Active Directory authentication logs (Security Event ID 4624/4625) for the 72-hour window surrounding document-open events to identify any lateral movement or credential use by the RAT operator — particularly relevant given the healthcare network targets where PHI access may trigger breach notification obligations under applicable data protection regulations.

## Detection Guidance

No confirmed IOCs (hashes, domains, IPs) are publicly available in current reporting. Detection must rely on behavioral and process-based indicators. (1) Email gateway: flag inbound messages with sender domains that closely resemble cert.gov.ua using lookalike detection (e.g., homoglyph substitution, subdomain abuse, free-mail impersonation). (2) Endpoint: alert on email client or Office application processes spawning scripting engines (cmd.exe, powershell.exe, mshta.exe, wscript.exe). (3) Network: detect low-frequency, regular-interval outbound HTTP or HTTPS connections from workstations to external hosts with no prior reputation baseline, consistent with RAT C2 beaconing (T1071.001). (4) Registry and persistence: monitor for new entries in HKCU\Software\Microsoft\Windows\CurrentVersion\Run and scheduled task creation outside of change windows. (5) Lateral movement: alert on T1078 indicators, account logons from new source hosts or at unusual hours following a suspected phishing event. Monitor CERT-UA's official advisory feed (cert.gov.ua) for published IOCs as the investigation matures.

## Indicators of Compromise

| Type | Value | Context | Confidence |
|---|---|---|---|
| DOMAIN | `cert.gov.ua` | Legitimate CERT-UA domain — included for reference to assist in identifying lookalike/spoofed sender domains, not as a malicious indicator | HIGH |

## Framework Mappings

### MITRE-ATTACK

- **T1219** — Remote Access Tools
- **T1071.001** — Web Protocols
- **T1036** — Masquerading
- **T1105** — Ingress Tool Transfer
- **T1566** — Phishing
- **T1078** — Valid Accounts
- **T1566.001** — Spearphishing Attachment
- **T1036.005** — Match Legitimate Resource Name or Location

### NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

### CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

### HIPAA-SECURITY

- **164.308(a)(5)(i)** — Security Awareness and Training
- **164.308(a)(6)(ii)** — Response and Reporting

### SOC2-TSC

- **CC7.4** — Responds to identified security incidents

### ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1219 | Remote Access Tools | Command-And-Control |
| T1071.001 | Web Protocols | Command-And-Control |
| T1036 | Masquerading | Defense-Evasion |
| T1105 | Ingress Tool Transfer | Command-And-Control |
| T1566 | Phishing | Initial-Access |
| T1078 | Valid Accounts | Defense-Evasion |
| T1566.001 | Spearphishing Attachment | Initial-Access |
| T1036.005 | Match Legitimate Resource Name or Location | Defense-Evasion |

## Sources

| Source | URL | Tier |
|---|---|---|
| **gemini** | https://thecyberexpress.com/hackers-impersonate-ukrainian-cert-to-p... | T3 |
| **Hackers hit Ukrainian state agencies, critical infrastructure with new ...** | https://therecord.media/hackers-ukraine-critical-infrastructure-mal... | T3 |

| Source | URL | Tier |
|---|---|---|
| **Attacks on Ukrainian healthcare facilities during the first year ... - PMC** | https://pmc.ncbi.nlm.nih.gov/articles/PMC10704854/ | T1 |
| **Ukraine witnessing increasing impact of attacks on health and ...** | https://www.who.int/europe/news/item/07-02-2024-ukraine-witnessing-... | T3 |
| **Russian Actors Use Compromised Healthcare Networks Against ...** | https://www.darkreading.com/threat-intelligence/russian-actors-comp... | T3 |

## DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-03-31 06:18 UTC by TJS Security Command Center